

May 9, 2022

By Electronic Mail

Vanessa A. Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

RE: File No. S7-09-22: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Submitted By: Joshua Mitts*

Dear Secretary Countryman:

The Commission should be commended for a thoughtful and comprehensive proposal to cybersecurity incident reporting. The Commission's proposed rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* ("the proposal"),¹ will protect investors by reducing information asymmetry and enhancing share-price accuracy in the capital markets. This letter applauds the Commission's attention to academic scholarship on informed cybertrading and respectfully raises a few specific comments the Commission may wish to consider before finalizing the proposal.

As the Commission recognizes, current reporting of cybersecurity risks is critical because mispricing resulting from delayed or incomplete cybersecurity incident disclosure can be dangerously exploited by informed cybertraders.² The implications of informed cybersecurity trading are distinct from garden-variety information trading in securities markets.³ Typically, new information is merely observed by an information trader; in informed cyber-trading, the new information may be substantially "created" and imposed on a firm by the same actors who cause a cybersecurity breach, or those acting in concert with them.⁴ Those actors may trade ahead of disclosure of a cybersecurity breach they caused.⁵ Allowing parties to capture profits generated from this type of trading, therefore, incentivizes cybertraders to exploit cybersecurity vulnerabilities in order to reap arbitrage gains following disclosure of a hack.⁶

Such information arbitrage opportunities catalyze destructive activity for the purpose of trading on the basis of the harm it creates – leading to greater dissemination of stolen personal information, impersonation, and identity theft.⁷ Because insider trading in connection with cybersecurity breaches presents economic costs largely absent in garden-variety information-trading, enhanced legal scrutiny of those who profit from the activity is plausibly justified.⁸ Yet, informed cybertraders are unlikely to face any liability under current law.⁹ As the Commission rightly identifies, it is therefore vital to ensure effective

* Associate Professor of Law and Milton Handler Fellow, Columbia Law School. The opinions expressed here are the author's alone.

¹ 87 FR 16590 (Mar. 23, 2022).

² 87 FR 16608.

³ Joshua Mitts & Eric Talley, *Informed Trading and Cybersecurity Breaches*, 9 HARV. BUS. L. REV. 1, 30-31 (2019).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* at 4.

⁸ *Id.*

⁹ *See id.* at 4, 38-40.

disclosure of cybersecurity risks.¹⁰ By mandating current reporting of cybersecurity incidents on Form 8-K, the proposal will foreclose opportunities to trade on the basis of undisclosed cybersecurity information.

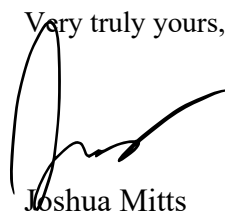
Before finalizing the proposal, the Commission may wish to consider the following comments to further strengthen the deterrent effect of the proposal on trading on material, nonpublic cybersecurity information. **First**, the Commission may consider prohibiting insider trading during the period of time after a firm's materiality determination but before disclosure through a public filing. Imposing a blackout period during the disclosure window would encourage firms to file 8-K reports quickly but preserve firms' ability to wait to make materiality determinations until they are able to provide accurate disclosures.

Alternatively, the Commission may consider shortening or eliminating the four-business day filing period for 8-K reports triggered by cybersecurity incidents. The problem of sanctioning delay before disclosing material events to investors is well-recognized.¹¹ The most compelling justification for preserving a four-day gap between the occurrence of a material corporate event and the Form 8-K filing deadline is that it takes time for companies to make a determination of materiality and prepare precise information. However compelling that justification may be, it should not apply to firms' reporting obligations under Item 1.05. Under the proposal, a firm's disclosure obligation would arise only when a cybersecurity incident is "determined by a registrant to be material."¹² Therefore, if a firm determines it needs additional time to prepare a disclosure, it could simply delay making a determination of materiality.

Second, the Commission may also wish to reconsider its inclusion of Item 1.05 as one of the Form 8-K items eligible for the safe harbor exemption from liability under Exchange Act 10(b) and Rule 10b-5. The stated justification for the safe harbor – that it is appropriate "if the triggering event for the Form 8-K requires management to make a rapid materiality determination"¹³ – is not as compelling for cybersecurity incident reporting. The Commission's proposal requires registrants to make materiality determinations only as soon as is "reasonably practicable after discovery of the incident."¹⁴ Registrants, therefore, need not make rapid materiality determinations to comply with the Commission's proposal, and shielding companies from potential liability stemming from reporting failures may weaken the effect of the proposal.

Finally, the Commission may wish to require that there be a reasonable basis for a firm's materiality determination to allow for *ex post* inquiry not only into the reasonableness of the timing of a firm's materiality determination but also into the reasonableness of the factual basis for the determination.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Joshua Mitts', with a stylized, sweeping flourish extending from the end of the name.

Joshua Mitts

¹⁰ 87 FR 16608.

¹¹ See Alma Cohen, Robert J. Jackson, Jr., & Joshua R. Mitts, *The 8-K Trading Gap* (Columbia L. Sch. Ctr. for L. & Econ. Stud. Working Paper No. 524, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657877 (demonstrating that insiders profitably trade between the time material events occur and when they are required to disclose market-moving information pursuant to the Commission's 8-K rules); H.R. 4435, 116th Cong. (2020) (Recognizing the "8-K trading gap" as troubling, in January 2020, the House of Representatives overwhelmingly passed legislation aimed at preventing corporate insiders from trading their securities after a significant corporate event but before disclosing that event through a Form 8-K filing.).

¹² 87 FR 16596.

¹³ 87 FR 16597.

¹⁴ *Id.*